DETAILED ACTION

Applicant amends claim 3.

Claims 1-3, 7, 8 and 11 are re-presented for examination.

Response to Arguments

Applicant's arguments, see Remarks, filed 07 June 2010, with respect to claims 1-3, 7, 8 and 11 have been fully considered and are persuasive. The previous grounds of rejection have been withdrawn.

1. Applicant argues on pages 6-7 of Remarks regarding Hollander: "However, nowhere in Hollander is there any disclosure or suggestion of determining whether the data includes instructions for a forward branch where the destination address of the forward branch is associated with a call instruction whose destination address is between the origin and destination address of the branch instruction as claimed."

The Examiner finds this argument persuasive and withdraws the claim rejections.

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Ms Penny Caudle on 14 June 2010.

The application has been amended as follows:

1. (Currently Amended) A data processing method including receiving input data containing a plurality of instruction codes, and judging whether or not a process executed based on the instruction codes contained in the received data is a malicious process, said method comprising:

sequentially reading, using a processor, one byte of the input data at a time;

determining, using a processor, whether or not the read data is a branch instruction;

~~if~~ when the read input data is a branch instruction, determining whether a branch destination address of the branch instruction is larger than a branch origin address based only on the one byte of the data read and ~~if the branch destination address is larger than the branch origin address~~ storing the branch destination address and branch origin address, when the branch destination address is determined to be larger than the branch origin address;

determining, using a processor, whether or not there is a call instruction at the branch destination address, and storing a call destination address of the call instruction ~~if~~when the instruction code at the branch destination address is a call instruction;

determining, using a processor, whether or not the stored call destination address is between the branch origin address and the branch destination address; and

~~if~~when the stored call destination address is between the branch origin address and the branch destination address concluding that the input data includes a malicious process.

2. (Currently Amended) A data processor including means for receiving input data containing a plurality of instruction codes, for determining whether or not a process executed based on the instruction codes contained in the received data is a malicious process, said data processor comprising:

means for sequentially reading one byte of the input data at a time;

means for determining whether the read data is a branch instruction;

~~if~~ when the read input data is a branch instruction, determining whether a branch destination address of the branch instruction is larger than a branch origin address based only on the one byte of the data read and ~~if the branch destination address is larger than the branch origin address~~ storing the branch destination address and the branch origin address when the branch destination address is determined to be larger than the branch origin address;

means for determining whether or not there is a call instruction at the branch destination address, and storing a call destination address of the call instruction ~~if~~ when the instruction code at the branch destination address is a call instruction; and

means for determining whether or not the stored call destination address is between the branch origin address and the branch destination address; and

~~if~~when the stored call destination address is between the branch origin address and the branch destination address concluding that the input data includes a malicious process.

3. (Currently Amended) The data processor as set forth in claim 2, further comprising means for judging whether or not a predetermined character string is associated with a return address of ~~the~~ an instruction code group called by the call instruction, wherein ~~if~~ when the predetermined character string is associated with the return address, the information indicating that the data is data for executing a malicious process is outputted.

7. (Currently Amended) A non-transitory computer-readable memory ~~product storing~~having stored thereon a computer program ~~including causing~~that causes a computer to judge whether or not a process executed based on input data containing a plurality of instruction codes is a malicious process, the stored computer program comprising code for causing a processor to:

~~causing the computer to~~ sequentially read one byte of the input data at a time;

~~causing the computer to~~ determine whether or not the read data is a branch instruction;

~~if the read input data is branch instruction, causing the computer to~~ determine whether a branch destination address of the branch instruction is larger than a branch origin address based only on the one byte of the data read, when the read input data is determined to be a branch instruction, and ~~if the branch destination address is larger than the branch origin address causing the computer to~~ store the branch destination address and branch origin address when the branch destination is determined to be larger than the branch origin address;

~~causing the computer to~~ determine whether or not there is a call instruction at the branch destination address and to store a call destination address of the call instruction ~~if~~when the instruction code at the branch destination address is a call instruction;

~~causing the computer to~~ determine whether or not the stored call destination address is between the branch origin address and the branch destination address; and

~~if the stored call destination address is between the branch origin address and the branch destination address causing the computer to~~ conclude that the input data includes a malicious process when the stored call destination address is determined to be between the branch origin address and the branch destination address.

8. (Currently Amended) A data processor comprising:

an input unit for inputting data containing a plurality of instruction codes;

a storing unit for storing the data input by the input unit; and

a controller capable of performing operations of;

sequentially reading one byte of the input data at a time;

determining whether or not the read data is a branch instruction;

~~if~~when the read data is a branch instruction determining whether a branch destination address of the branch instruction is larger than a branch origin address based only on the one byte of the data read, and ~~if the branch destination address is larger than the branch origin address~~ storing the branch destination address and branch origin address when the branch destination address is determined to be larger than the branch origin address;

determining whether or not there is a call instruction at the branch destination address and storing a call destination address of the call instruction in the storing unit ~~if~~when the instruction code at the branch destination address is a call instruction;

determining whether or not the stored call destination address is between the branch origin address and the branch destination address; and

~~if~~when the stored call destination address is between the branch origin address and the branch destination address concluding that the input data includes a malicious process.

Allowable Subject Matter

Claims 1-3, 7, 8 and 11 are allowed.

The following is an examiner's statement of reasons for allowance:

The prior art does not teach nor in combination suggest a data processing method including receiving input data containing a plurality of instruction codes, and judging whether or not a process executed based on the instruction codes contained in the received data is a malicious process, said method comprising: sequentially reading, using a processor, one byte of the input data at a time; determining, using a processor, whether or not the read data is a branch instruction; when the read input data is a branch instruction, determining whether a branch destination address of the branch instruction is larger than a branch origin address based only on the one byte of the data read and storing the branch destination address and branch origin address, when the

branch destination address is determined to be larger than the branch origin address; determining, using a processor, whether or not there is a call instruction at the branch destination address, and storing a call destination address of the call instruction when the instruction code at the branch destination address is a call instruction; determining, using a processor, whether or not the stored call destination address is between the branch origin address and the branch destination address; and when the stored call destination address is between the branch origin address and the branch destination address concluding that the input data includes a malicious process.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to DARREN SCHWARTZ whose telephone number is (571)270-3850. The examiner can normally be reached on 7am-4pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571)272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/D. S./
Examiner, Art Unit 2435
/Kimyen Vu/
Supervisory Patent Examiner, Art Unit 2435